REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested.

Claims 1-10, 12-32 and 35-43 are pending in the present application. Claim 1 has been amended to include the limitation of now-canceled dependant claim 11. Claim 29 has been amended to include the limitation of now-canceled dependant claims 33 and 34. Accordingly, claims 11, 33 and 34 have been canceled.

Claim 31 was amended in accordance with the Examiner's suggestion. Regarding claim 35, Applicant requests the Examiner to clarify the correction that is required.

The rejection of claims 1-48 under 35 USC 102 (e) as being anticipated by Moran (U.S. patent 6,647,400) is hereby traversed. A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. The Examiner has failed to identify all elements of amended claim 1 as anticipated by the Moran reference.

With respect to claim 1, Moran fails to disclose the use of a memory mapped file as required by the subject matter of claim 1. The examiner asserts that Moran, at column 9, line 54-column 10, line 32 and column 22, line 65-column 23, line 3, discloses a memory mapped file; however, the examiner is incorrect as the identified location does not describe the use of a memory mapped file. Moran describes the data collection modules as separate programs people to send information to another computer for analysis without specifying the use of a memory mapped file. In fact, Moran appears to rely on hope will for preventing the compromise of the transmissions, e.g., "send the extracted information to another (hopefully uncompromised) computer for analysis" column 10, lines 17-19. The second examiner-identified location (column 22, line 65-column 23, line 3) merely refers to a description of the the cron and at deamons available on some operating systems. There is no discussion of a memory mapped file at this location.

Further, the examiner-identified portion of Moran fails to explicitly recite the reading of kernel records and/or reformatting the read kernel records into a different format and/or parsing

and comparing the kernel records against a template. Moran describes extracting data from system logs and other files, but fails to describe the use of kernel records.

For either of the foregoing reasons, Moran fails to anticipate the claimed subject matter of claim 1 and the rejection should be withdrawn. Claims 2-10, 12-28 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over Moran for at least the reasons advanced above with respect to claim 1 and the rejection should be withdrawn.

Further, and with specific reference to claim 9, The examiner-identified portion of Moran fails to describe encrypting information sent between the intrusion detection system and a network. Moran at column 16, lines 15-29 merely describes the passing of values between components of the system using encoding and decoding of data items, e.g., performing data type conversions, but this is not the same as encrypting the information sent as claimed and claim 9. Moran fails to describe the encryption of information transmitted at any point of the process. For at least this reason and the reasons advanced above with respect to claim 1 from which claim 9 depends, the rejection of claim 9 should be withdrawn.

With respect to claim 28, Moran fails to disclose the specifics of the subject matter of claims 33and 34 now incorporated into claim 29, i.e., if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored and that the predetermined set of files includes a system kernel file and system kernel configuration files. Similar to the above-described arguments with respect to claim 1and the lack of the teaching of reading kernel records by Moran, Moran fails to describe monitoring a system kernel file and system kernel configuration files. As described above with respect to claim 1, system log files may be read; however there is no description of system kernel files and/or system kernel configuration files. Further, Moran fails to describe the specific directory and file exclusions specification as claimed in claim 29. In the examiner identified portion of Moran, particular directories and files to be checked are specified, but there is no description of the specifics of file and directory checking interaction when dealing with exclusions.

For either of the foregoing reasons, Moran fails to anticipate the claimed subject matter of claim 29 and the rejection should be withdrawn. Claims 30-32 and 34-43 to attend, either directly or indirectly, from claims 29, include further important limitations, and are patentable

over Moran for at least the reasons advanced above with respect to claim 29 and the rejection should be withdrawn.

The rejection of claims 11, 33-34 and 44-48 are moot in view of the above cancellation of these claims.

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN & BERNER, LLP

Randy A. Noranbrock
Registration No. 42,940

Customer Number: 22429
1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: January 18, 2005
KMB/RAN/iyr